UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/646,640	11/09/2000	Patrick Salle	76.0481	1842

41754 7590 09/28/2005

PEHR JANSSON, ATTORNEY AT LAW
7628 PARKVIEW CIRCLE
AUSTIN, TX 78731

EXAMINER	
KIM, JUNG W	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 09/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/646,640	SALLE, PATRICK	
	Examiner	Art Unit	
	Jung W. Kim	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 August 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *10-15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *10-15* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 August 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This Office action is in response to the amendment filed on August 18, 2005.

2. Claims 10-15 are pending.

3. Claim 10 is amended.

4. Claims 14 and 15 are new.

5. Claims 1-9 are canceled.

Continued Examination Under 37 CFR 1.114

6. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on August 18, 2005 has been entered.

Response to Arguments

7. Applicant's arguments with respect to amended claims 10-13 have been considered but are moot in view of the new ground(s) of rejection.

Drawings

8. The drawings were received on August 18, 2005. These drawings are acceptable.

Claim Objections

9. Claim 13 is objected to because the limitation of claim 13 does not appear to further limit the parent claim; the limitation of "wherein the modification of the order of execution of operations is random" in claim 13 appears as "randomly modifying the order of execution of operations" in claim 10.

Claim Rejections - 35 USC § 112

10. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

11. Claims 11 and 12 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

12. Claim 11 recites the limitation "permutation of bits of a message block" and "permutation of bits of a key". There is insufficient antecedent basis for these limitations in the claim.

13. Claim 12 recites the limitation "the order of processing quartets making up a data element". There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 101

14. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

The claimed invention is non-statutory since it is not tangible. The methods recited in claims 10-15 define a data protection method wherein executing operations within the encrypting method are reordered or randomized. However, none of the steps require the use of hardware, and hence the claims are deemed non-statutory.

Claim Rejections - 35 USC § 103

15. Claims 10-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over FIPS PUB 46-2 "Data Encryption Standard" (hereinafter FIPS 46-2) in view of Collberg et al. "A Taxonomy of Obfuscting Transformations" (hereinafter Collberg).

16. As per claim 10, FIPS 46-2 discloses a data protection method (DES), the method using a cryptographic algorithm for executing operations for processing data elements so as to generate encrypted information. DES is a symmetric algorithm implementing an initial permutation, a key transformation (including key permutation), an expansion of data into quartets, s-box substitution, a p-box permutation, and then a final permutation; the key transformation, expansion of the data into quartets, s-box substitution and p-box transformation occur per round for 16 rounds. In addition, software implementation of DES is sanctioned (see entire document).

17. FIPS 46-2 does not disclose randomly modifying the order of execution of operations from one cycle to another, a cycle being a complete execution cycle of the algorithm or an intermediate cycle of a group of operations, the operations being

operations whose order of execution relative to the others does not affect the result. Collberg discloses a method of preventing trade secrets from being uncovered using obfuscation transformations. Obfuscation transformations are defined as a transformation of a source program to a target program such that the source program and target programs have the same observable behavior (pg. 6, Definition 1). Collberg discloses two such transformations: using loop unrolling and reordering steps to mask the operations of a program (pgs. 10-17, section 6, especially section 6.3.4 and 6.4). In the case of a program like DES, unrolling the 16 rounds and randomizing the order of execution are obvious constructions; many of the operations relative to one another within each round are commutative. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to randomly modify the order of execution of operations from one cycle to another, a cycle being a complete execution cycle of the algorithm or an intermediate cycle of a group of operations, the operations being operations whose order of execution relative to the others does not affect the result, since obfuscation transformation prevents reverse engineering (Collberg, Abstract). Note, the "thereby" clause in the claim does not limit the claim to a particular structure and hence does not limit the scope of the claim. MPEP 2106.II.C. The aforementioned cover the limitations of claim 10.

18. As per claims 11 and 12, the rejection of claim 10 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, the reordering of the execution of the permutation of the message block and the execution of the permutation of the key, as

well as the reordering of the processing quartets that make up a data element, are obvious enhancements, since the operations are commutative, and reordering steps of a program masks the operation of the program, which prevents reverse engineering (Collberg, Abstract; section 6.4).

19. As per claim 13, the rejection of claim 10 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, the modification of the order of execution of operations is random (Collberg, pg. 16, section 6.4 "Ordering Transformations").

20. As per claim 14, FIPS 46-2 discloses a data protection method (DES), the method using a cryptographic algorithm for executing operations for processing data elements so as to generate encrypted information. DES is a symmetric algorithm implementing an initial permutation, a key transformation (including key permutation), an expansion of data into quartets, s-box substitution, a p-box permutation, and then a final permutation; the key transformation, expansion of the data into quartets, s-box substitution and p-box transformation occur per round for 16 rounds. In addition, software implementation of DES is sanctioned (see entire document).

21. FIPS 46-2 does not disclose a random determination of a processing order of the bits for the execution of the permutation step. Collberg discloses a method of preventing trade secrets from being uncovered using obfuscation transformations. Obfuscation transformations are defined as a transformation of a source program to a target program such that the source program and target programs have the same

observable behavior (pg. 6, Definition 1). In particular, Collberg discloses a transformation of reordering steps to mask the operations of a program (pg. 16, section 6.4 "Ordering Transformations"). In the case of a program like DES, randomizing the order of operations are obvious constructions; many of the operations relative to one another within each round are commutative. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to make a random determination of a processing order of the bits for the execution of the permutation step, since obfuscation transformation prevents reverse engineering (Collberg, Abstract). Note, the "thereby" clause in the claim does not limit the claim to a particular structure and hence does not limit the scope of the claim. MPEP 2106.II.C. The aforementioned cover the limitations of claim 14.

22. As per claim 15, the rejection of claim 14 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, the cryptographic algorithm for executing operations for processing data elements includes a group of operations executed repeatedly (DES has 16 rounds).

Conclusion

23. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

24. Kocher USPN 6,327,661.

Communications Inquiry

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W. Kim whose telephone number is 571-272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jung W Kim
Examiner
Art Unit 2132

September 23, 2005

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100